GESTIÓN DE RIESGOS EN EL INTERNET DE LAS COSAS (IoT)

Gantiva Henao, Luis Alexander
gantivared@gmail.com
Universidad Piloto de Colombia - Esp. Seguridad Informática
Bogotá, Colombia

***Resumen*—** Este artículo es una referencia para realizar una gestión de riesgos y adaptarlo a Internet de las cosas (IoT) con base a estándares de seguridad, entre los cuales se encuentran, ISO27001, marcos de referencia de ISO31000 y metodologías como Magerit. Explica acerca de la gestión de riesgos que tendrán los dispositivos y servicios llamados cosas, analizando el contexto empresarial y del entorno del usuario para el uso correcto del dispositivo en el IoT, con el propósito final de proteger la información del usuario, de la falta de disponibilidad, de integridad y de confidencialidad del usuario en la nube o en Internet.

***Abstract*—** This article is a reference to carry out risk management and adapt it to the Internet of Things (IoT) based on security standards, among which, ISO27001, ISO31000 reference frameworks and methodologies such as Magerit. It explains about the risk management that devices and services called things will have, analyzing the business context and the user's environment for the correct use of the device in the IoT, with the final purpose of protecting user information, from the lack of availability, integrity and confidentiality of the user in the cloud or on the Internet.

***Índice de Términos*—** Acciones de riesgo, Internet de las cosas, Inventario de activos, Valoración de amenazas.

I. INTRODUCCIÓN

Este documento es una referencia de cómo se puede adaptar una gestión de riesgos en el internet de las cosas, llamado en ingles *Internet of Things* (IoT). Trata de explicar los riesgos que pueden tener en los distintos dispositivos que se encuentran enlazados en internet, ya sean de uso corporativo o de uso personal y cómo mitigar estos riesgos, realizando una adecuada gestión de riesgos que proteja en gran medida la disponibilidad, la integridad y la confidencialidad de la información del usuario en el *Internet de las cosas*.

II. QUÉ ES EL INTERNET DE LAS COSAS

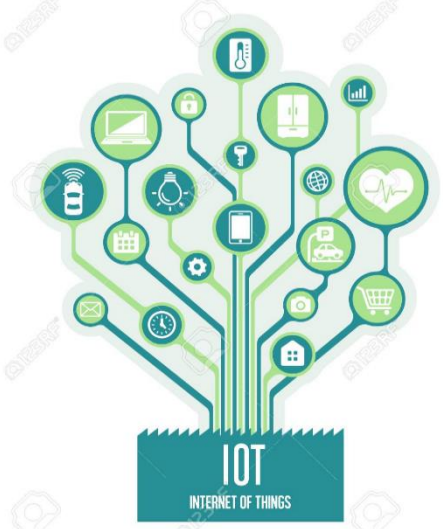
El Internet de las cosas o en ingles *Internet of Things* (IoT) es un sistema que interrelaciona en el internet o en la nube, dispositivos de cómputo, maquinas digitales, objetos caseros, robótica, animales y/o persona con identificadores únicos, sistemas domóticas y etc.

Una mejor definición del IoT es realizada por la IEEE: *"Internet de las cosas (IoT): Es una red cableada o inalámbrica de dispositivos conectados identificables de manera única que pueden procesar datos y comunicarse entre sí con o sin participación humana"* [1]. Todo dispositivo o sistema conectado a una red, ya sea cableada e inalámbrica, que tenga algún propósito funcional y adicional, que se encuentre en comunicación dentro de la nube o internet, se le llama Internet de las cosas (IoT).

El concepto del Internet de las cosas fue creada por Kevin Ashton en 1999 para entonces, era un gerente de la compañía Procter and Gamble (PyG). "Ashton trataba de resolver un problema, que los productos más populares de PyG no se encontraban disponibles en la tienda, descubrió que eso ocurría que a mayor publicidad de un producto, más rápido se agotaba, la solución era poner sensores conectados a la red de los productos PyG y saber cuándo se agotaban" [2].

Ashton, utilizó el acrónico IoT, para identificar, dispositivos o "cosas" que utiliza el internet cómo medio disponible de comunicación en un sistema tecnológico.

Figura1- Ejemplo de árbol de conexión de las cosas de IoT



Fuente: https://www.shutterstock.com/es/image-vector/iot-internet-things-illustration-tree-blue-783132853

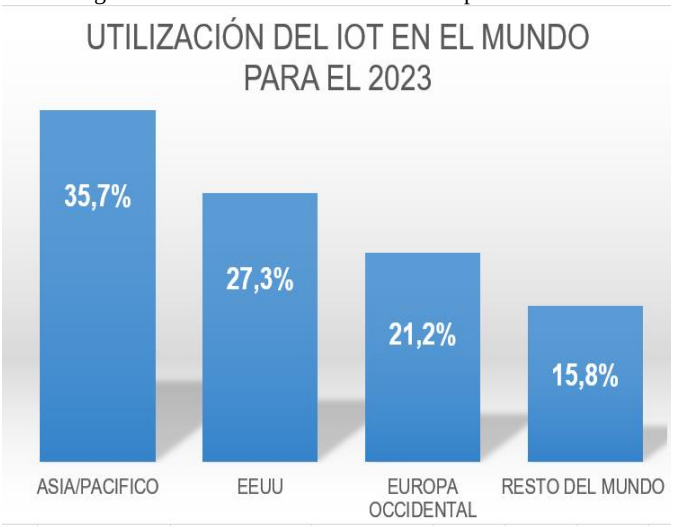
III. IMPORTANCIA DEL IoT

El internet hoy en día, se encuentra en dispositivos distintos a los teléfonos inteligentes, donde se puede acceder a los datos personales, a información confidencial, a información pública o a información privada; el internet también se encuentra en dispositivos inteligentes cómo neveras, lavadoras, televisores, elementos de cocina, sensores, actuadores, pueden acceder a las redes sociales, al e-mail corporativo, al e-mail personal o se puede acceder a un servicio de nube de alojamiento de archivos cómo dropbox o drive de google, por lo tanto, son dispositivos que contienen o trasmiten información relevante, asegurar estos elementos o cosas debe ser primordial para quienes lo utilicen. Al usuario de estos dispositivos se le debe crear conciencia y a enseñarle buenas prácticas de seguridad para que proteja su información, si no se le da un buen tratamiento, puede generar algún impacto que no desearía tener y consecuencias que no quisiera asumir.

El concepto de IoT ha llegado para interconectar cualquier dispositivo o "cosa" al internet, por eso según pronóstico de *IDC (International Data Corporation)* estima que para el 2025 se encontraran conectados al IoT alrededor de 41.6 billones de dispositivos generando 79.4 zettabytes (ZB) [3], estos dispositivos son de uso multidisciplinario, se pueden encontrar para el uso personal, el hogar, la industria, el comercio, medicina, entidades financieras, transporte, servicios, anímales y etc.

IDC también prevé que para el año 2023 el gasto de internet de las cosas tan solo en Asia/Pacifico alcance los USD 398,6 mil millones de dólares, liderando a nivel mundial el gasto del internet de las cosas con alrededor del 35.7% seguido por los Estados Unidos de América y Europa Occidental con el 27.3% y el 21.2% respectivamente [4].

Figura 2- Grafica de utilización del IoT para el 2023



Fuente: El autor

Considerando estas cifras, se puede interpretar que el crecimiento del internet de las cosas no solo va a permitir una gran oportunidad económica, también se va a convertir en una súper autopista en donde va a recorrer una gran cantidad de información, no solo se va a encontrar comunicación entre dispositivos, si no también, son datos que se encuentran almacenados en muchos lugares en la nube y en el mundo.

Como en cualquier idea, siempre se tiene pensado en un cambio importante que beneficie a una población, una idea revolucionaria, no solo cambia la forma de pensar, también revoluciona las costumbres, mejora y hace más sencilla la vida de las personas. Para IoT el beneficio más importante es que los procesos sean automatizados, agiles, eficientes y disponibles, que generen algún tipo de valor, ya sea una mejor calidad de vida o se obtenga un crecimiento financiero para distintos negocios, por tal motivo, se debe considerar las ventajas y las desventajas que se tiene hasta el día de hoy del Internet de las cosas, pues la información se puede convertir en un activo que puede generar ganancia o por el contrario, se puede convertir en un activo que puede generar pérdidas.

Es indiscutible el impacto que traerá las cantidades de dispositivos que se encuentren interactuando en el IoT, ocasionará impactos positivos o negativos y tanto a empresas como a usuarios no desearían tener ningún tipo de pérdida en el uso de un servicio de IoT. Siempre, cuando se adquieren una solución o se ingresa a un mundo desconocido en la tecnología, se desea obtener algún tipo de valor, ya sea monetario o un valor que beneficie y mejore la calidad de vida, para así poder sacar el mayor provecho posible a un nuevo servicio tecnológico.

A. Ventajas de IoT

Se encuentran varias ventajas que las empresas y los usuarios le pueden sacar la mayor ventaja al uso de los dispositivos del IoT, para ello se nombran algunas que pueden ser las más relevantes de este universo.

1) Comunicación M2M: es una comunicación que se realiza entre dispositivos o entre maquinas conocida como M2M (machine to machine), los dispositivos pueden permanecer conectados entre sí y solicitar órdenes en una ejecución automática, por ejemplo: Un sistema novedoso cómo el que se encuentra en las tiendas Amazon (no filas no cajeros) las estanterías de su mercancía automáticamente identifican en que fila o hilera ha sido tomado el producto, este sistema cuenta con sensores que realiza la identificación de la cantidad de mercancía que se encuentran en exhibición, pero primero ¿qué pasa si esta mercancía está a punto de terminarse? segundo ¿Qué pasa si el cliente toma la mercancía y lo ingresa a la canasta de compra? Para ello existen las líneas M2M, los sensores de las estanterías se comunican con un servidor central llamado también gateway, para el primer caso, identifica que la mercancía se encuentra por acabarse y necesita ser abastecido en la estantería, generando una alarma en un centro de monitoreo al encargado de surtir la mercancía. Para el segundo caso, el servidor central se encuentra en comunicación con los sensores de los exhibidores y adicional, identifica la ubicación del comprador en la tienda; el sensor en comunicación con el gateway, identifica que mercancía tomó e ingresó en la canasta el comprador, para así automáticamente ir sumando el precio en

un aplicativo web o de celular los productos que se encuentran en la canasta.

2) Automatización: Debido a que las máquinas se encuentran conectadas entre sí y controladas por un servidor central, realizan procesos automatizados con código lógico, programados por medio de un software de IA (Inteligencia artificial) que no es necesario la intervención humana, así, reduciendo tiempo en los procesos repetitivos y economizando gastos adicionales en mano de obra.

3) Información y análisis de datos: Cuando hay sistemas automáticos, se encuentra suficiente información para que el proceso a realizar sea más eficiente, pues los componentes de un sistema tienen una gran habilidad de análisis de los datos recopilados para tomar las decisiones correctas. Esta capacidad que tiene un sistema automático en el IoT, dispone de la habilidad de almacenar los datos suficientes para mejorar, un sistema de tratamiento médico, un sistema que ayude a un estudio de mercado o en un sistema que deba tomar la decisión para realizar una compra.

4) Monitoreo: Los sensores interconectados en los diferentes sistemas automáticos que se encuentran en el IoT, permite monitorear constantemente un proceso. Suponiendo un sistema de tratamiento médico, a un paciente se le pudo haber agotado el medicamento que se almacena en un dispositivo de IoT, inmediatamente, por medio de un aplicativo web o de celular, hará una advertencia indicando que el medicamento se ha acabado y se debe comprar ya sea personalmente o si lo prefiere, el dispositivo de IoT hará la compra para que le llegue a domicilio al hogar del paciente.

5) Ahorro de Tiempo: La ventaja de los procesos automatizados es el ahorro del tiempo para tomar una decisión o analizar una información, cómo en el siguiente caso: Una nevera inteligente, tiene la capacidad de saber que producto se haya terminado o esté a punto de acabar, la nevera puede solicitar la compra de ese producto de acuerdo a una programación inicial que le haya realizado el usuario o, la nevera avisa al usuario por medio de un aplicativo de celular, indicando que el producto se ha terminado y debe acercarse a la tienda más cercana, o si le da la autorización de realizar la compra; en este caso, la nevera le ha ahorrado tiempo al usuario porque justo ese día no podía acercarse al supermercado.

6) Dinero: Así como en el caso del punto anterior se narró un ejemplo de ahorro de tiempo, también se ahorró dinero, con todos los datos y la información recopilada, la automatización del sistema toma las decisiones en un proceso, puede ahorrar dinero ya que el dispositivo o el sistema va a tomar la mejor decisión para que no tenga afectación económica al usuario, la nevera le puede preguntar al usuario quien realiza la compra, si el sistema o él usuario.

7) Mejor calidad de vida: las aplicaciones de IoT tienen control de procesos automatizados que a la vez, le permite al usuario tener una mejor calidad de vida, suprimiendo cargas innecesarias, por ejemplo, toma de decisiones que al usuario le puedan ocasionar algún tipo de estrés, decisiones que puedan quitar tiempo para pasar con su familia, el beneficio de tomar el transporte público a tiempo, monitorear su estado de salud, o pensar y hacer cosas más importantes que le puedan brindar felicidad.

B. Desventajas del IoT

Antes de que se tome la decisión de adquirir un servicio o un dispositivo que se encuentre en el *internet de las cosas*, debe hacer una valoración de las desventajas, esto con el fin de aceptar el riesgo que puede tener al hacer uso de estos dispositivos o servicios.

1) Compatibilidad: Muchos de los dispositivos y sensores no tienen un standard compartido y dependen de aplicaciones y desarrollos indicados por cada compañía de soluciones IoT, esto quiere decir, que se debe hacer la adquisición con un solo proveedor o marca de soluciones, en tal caso si se tiene pensado adquirir dispositivos y servicios de procesos automatizados de IoT, debe considerar que debe hacer la adquisición con una sola marca.

2) Complejidad: Puede resultar no solo complejo el uso del IoT, también puede presentar múltiples fallas, que un mal comando u orden ejecutada por el usuario haga que falle el sistema de IoT y realiza una ejecución automática no deseada, esto puede incurrir en gastos económicos no previstos y puede llegar el usuario a desanimarse con el sistema o servicio.

3) Seguridad y privacidad: Se convierte en un riesgo los datos e información personal que se pueda encontrar en cada dispositivo que haga parte del servicio de IoT; cabe la posibilidad de estar en constante amenaza la privacidad de una persona o usuario, ya que es susceptible al estar expuesta la información en el internet o en la nube. Puede ocurrir que los dispositivos o servicios adquiridos para uso de IoT, no se encuentren homologados en calidad y en seguridad, los fabricantes no les hayan realizado pruebas de penetración o de fallos de código de desarrollo, y en vez de convertirse este servicio en una solución, se puede convertir en un problema e inconveniente para el usuario o para la compañía.

*4) Susceptible a altas latencias: S*e puede presentar que el proveedor de servicio de internet o ISP tenga una falla de lentitud en el canal de internet, ocurre que en un sistema de IoT, las órdenes enviadas a los sensores no lleguen a tiempo y esto pueda incurrir en una falla de un proceso automatizado que se tenga , puede enviar ordenes desfasadas o incorrectas desde el servidor central a los sensores y actuadores, podría "enloquecer" el sistema o dispositivo y dañar la integridad de la información.

5) Indisponibilidad: De nuevo el usuario debe considerar que el uso de IoT puede resultar complejo si entiende poco o nada de tecnología, o no entender cómo es el funcionamiento y comportamiento de una red de datos. Los dispositivos y los proveedores de servicios de internet ISP´s no se encuentran blindados a fallos y cuando estos ocurren, puede ocasionar indisponibilidad del servicio y por ende, indisponibilidad en un sistema de IoT. Para el usuario o para una compañía que haya contratado dispositivos de IoT, no querrá escuchar que hubo un fallo en su sistema por motivos de indisponibilidad, pero es una desventaja que posiblemente no es controlable y que se puede presentar en cualquier instante.

6) La tecnología puede tomar control de su vida: Esto no quiere decir que la tecnología haya evolucionado para hacerle daño a las personas, pero si puede ocasionar en crearle un mal hábito al ser humano y convertirlo dependiente. Las personas pueden utilizar equivocadamente la tecnología cómo un arma o una herramienta que pueda hacer daño o le de algún beneficio, saltándose los requerimientos éticos y morales. Es verdad que la tecnología ha sido hecha e inventada para solucionar problemas cotidianos y mejorar la calidad de vida, pero hay que recordarle al usuario, que la tecnología ha sido realizada por humanos y no está susceptible a fallas y equivocaciones, por lo tanto, se debe tener cuidado en su utilización y manipulación, que estos servicios aún dependen del control y ordenes iniciales realizadas por el usuario, que han sido adquiridos para un beneficio en particular, tener la capacidad de análisis inicial de lo que se pretende hacer con el dispositivo o que proceso quiere realizar, se debe tener monitoreado cada acción o ejecución de un sensor o actuador que haga parte de un sistema de internet de las cosas, y no puede dejar en manos de la tecnología la responsabilidad moral que debe tener los seres humanos.

IV. GESTIÓN DE RIESGOS DE IoT

Las personas o las empresas se deslumbran cuando les hablan y les muestran nuevas tecnologías o nuevos servicios tecnológicos, y por lo general, las compañías de servicios o los proveedores de dispositivos que ofrecen el servicio de IoT, no hacen recomendaciones iniciales en seguridad para adquirir o elegir el dispositivo correcto, por eso este documento da una información general pero detallada, para tener en cuenta en la realización de una adecuada *gestión de riesgos de internet de las cosas*.

Inicialmente, se debe entender que es el riesgo, y es la probabilidad de que se produzca un contratiempo, un evento o una consecuencia negativa; el riesgo también es una magnitud de medida de daños frente a una situación de peligro. Estos riesgos se pueden aceptar, transferir, evitar y eliminar, se debe llevar el riesgo al punto más mínimo de que una eventualidad ocurra.

La nube o el internet siempre ha sido el caldo de cultivo de nuevas amenazas que pueden vulnerar la información de los usuarios o dispositivos, también es el lugar indicado para enviar códigos maliciosos a sistemas o dispositivos que se encuentren utilizando los usuarios y proveedores de servicios de IoT, un atacante puede vulnerar la seguridad de una infraestructura para poder robar y secuestrar la información. Cómo se ha indicado en los párrafos anteriores, el uso del *Internet de las Cosas* puede tener una serie de complejidad con el correcto uso de la seguridad, los usuario pueden desconocer las vulnerabilidades de los servicios y de los dispositivos que utiliza, pero los proveedores y fabricantes antes de ofrecer sus productos, deben suministrar la información suficiente y necesaria de los riesgos y oportunidades que va a tener con la adquisición de su servicio o dispositivo, tanto a nivel de calidad, o también suministrar información de las características del dispositivo a nivel de seguridad.

Las compañías que se encuentren en la posición de proveedor o cómo cliente, deben definir primero la documentación que les pueda ayudar a realizar una adecuada gestión de riesgos de IoT, elegir estándares reconocidos en la gestión y valoración de riesgos cómo la norma ISO/IEC 31000:2018 o hacer uso de metodologías que los oriente y los ayude a gestionar el riesgo correctamente, por ejemplo la metodología magerit. Para una empresa que se encuentre con una adecuada política de seguridad de la información cómo la ISO/IEC 27001:2013 no le va a ser difícil gestionar su riesgo, pues debe aplicar la cláusula 8.2 Evaluación de riesgos de seguridad de la información [5], 8.3 Tratamiento de riesgos de seguridad de la información [6] o adicional, puede usar los controles de la norma ISO/IEC 27017 *Controles de Seguridad para servicios Cloud y para la protección de los datos*. Para una adecuada Evaluación de riesgos en la nube puede hacer uso de la norma ISO/IEC 27018, estos controles son complementos de la norma ISO/IEC 27001:2013. Estas herramientas ayudan a la compañía a gestionar la seguridad y riesgo en la nube, permite aclarar las reglas de juego de los servicios IoT entre proveedor y usuario y adicional permite garantizar la seguridad del dispositivo o servicio.

Para los usuarios que no se encuentran con ningún compromiso empresarial y que independientemente han adquirido un dispositivo o servicio de IoT, es un poco más difícil y complicado de gestionar, pues muchas veces en una venta de dispositivos o servicios de IoT, los proveedores o fabricantes de marcas, no se hacen responsables de la información que le suministran al comprador del correcto uso del dispositivo de IoT, el usuario no tiene el conocimiento legal o técnico para exigir al proveedor que cumpla con las exigencias mínimas de seguridad. Cómo siempre ha ocurrido, las nuevas tecnologías van a un paso delante de los temas legales que puedan ocurrir después de una adquisición tecnológica, y los entes gubernamentales correspondientes los toman cómo casos de mejoras o lecciones aprendidas para modificar alguna ley, pero estas medidas se toman infortunadamente después de haberle causado algún tipo de daño material o moral al usuario, y no antes, cómo debería de ser; estas implicaciones son difíciles de controlar y analizar desde la etapa de inicio de desarrollo de un sistema, pero se pueden tomar como base los principios básicos de la seguridad, protegiendo inicialmente la confidencialidad, la integridad y la disponibilidad de la información.

Mientras hayan países que solucionen el tema legal para reglamentar el uso de cosas o dispositivos de servicio de IoT, se deben tomar algunas precauciones elementales, pues cómo se ha dicho anteriormente, para gestionar el riesgo a un usuario independiente no es sencillo, pero se deben crear algunos modelos informativos y preventivos del correcto uso de la seguridad del dispositivo o servicio de IoT, o tomar medidas que garanticen no solo el correcto funcionamiento del dispositivo o sistema si no también, que el dispositivo o sistema se encuentre con las condiciones mínimas de protección de la información del usuario.

A los usuarios no les es fácil identificar que dispositivo de IoT protege mejor su información, pero se tienen ejemplos de dispositivos cómo el uso de los celulares, que aunque el usuario

cuando compra su dispositivo telefónico no se le informa acerca de los riesgos y el buen uso del dispositivo en cuanto a seguridad, sí ha ido aprendiendo en la importancia de que este dispositivo si no se le da un correcto uso, puede ser vulnerada su información y privacidad. Hoy en día, muchas marcas del mercado son reconocidas por una buena reputación de seguridad en sus dispositivos, que con el tiempo, los usuarios las han ido identificando y adquiriendo por su buena percepción; pero esta buena reputación de los fabricantes de estos dispositivos, han sido reconocidos gracias a la publicidad y calidad de sus productos, pues estas marcas, han hecho una gran inversión económica en la identificación de las vulnerabilidades y riesgos que pueden tener la información de sus usuarios en sus dispositivos, en cierta medida, la protección y su correcto uso de la información no ha sido tan solo un valor agregado de aprendizaje para el usuario, si no también, han aprendido sus competidores, ofreciéndole a sus clientes una capacitación constante en seguridad de sus datos. Si nos damos cuenta, hoy en día muchos de los usuarios de los teléfonos celulares bloquean el inicio de sus pantallas cómo control mínimo de protección de su privacidad que le brinda su propio dispositivo, utilizan PIN, identificación de huella o de iris, patrones de desbloqueo y etc.

Así mismo, hoy en día con el uso del celular, muchas personas han aprendido y han tomado buenos hábitos para proteger la privacidad de sus datos; la mayoría de usuarios, tienen conocimiento y han tomado conciencia de la importancia de la seguridad que deben aplicar en sus aparatos tecnológicos, no obstante, están en la obligación los fabricantes y proveedores de aplicativos y de dispositivos de IoT, crear una mayor conciencia de un buen uso de los productos que ofrecen. Los fabricantes y proveedores deben alinear sus productos de IoT con las políticas internas de seguridad de la información que utilizan en su compañía y conocer los requerimientos legales de cada país en donde ofrecen sus servicios, deben tener una correcta gestión de riesgo de la información, para garantizarle al usuario que el dispositivo cuenta con estándares que cumplen con los requerimientos máximos de seguridad que protegen la información de sus datos, minimizar el riesgo de acuerdo a los controles de seguridad de la información que tiene aplicado el dispositivo o el sistema de servicio de IoT.

A continuación, se va a indicar los pasos y procesos para generar una adecuada gestión de riesgos, que permita y le sirva a los usuarios del Internet de las cosas (IoT).

A. Identificación del contexto

1*) Identificación del contexto de una compañía*: para una compañía el riesgo es distinto que para un usuario que adquiere independiente un dispositivo de IoT. Una compañía debe contar con políticas de seguridad de la información, por tal razón se debe regir a sus lineamientos corporativos. En el universo del IoT cuando se vaya a hacer uso de los servicios y de los dispositivos, lo primero que se debe realizar es identificar el contexto, cómo lo indica el IEC/ISO 27001 en la cláusula 4 "La organización debe determinar los problemas externos e internos que son relevantes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de seguridad de la información. NOTA La determinación de estos problemas se refiere al establecimiento del contexto externo e interno de la organización." [7].

Adicional, en la ISO 31000:2018 Gestión de Riesgo, indica el Marco de referencia o Frameworks cómo un factor de integración de riesgo a todas las funciones y procesos de la compañía con el compromiso y liderazgo de la alta dirección y de los organismos de supervisión.

Cómo se indica en el marco de referencia 5 de "Diseño de la ISO 3100:2018" también se encuentra la referencia 5.4 "Comprender la Organización", que dice: "Al diseñar el marco para gestionar el riesgo, la organización debe examinar y comprender su contexto externo e interno."[8].

Figura3- Framework Iso 31000:2018

Fuente: ISO 31000:2018 Cláusula 5

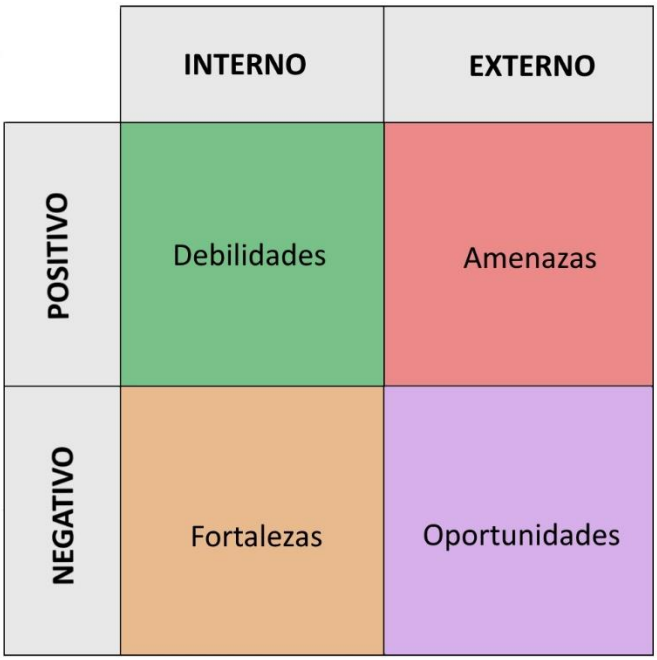
Para la identificación del riesgo, el primer paso es identificar el Contexto, este debe ser identificado tanto interno como externo. Para identificar el contexto externo incluye el lugar donde se encuentra la compañía (ciudad, país o zona) y los factores que la implican, entre los cuales: la cultura del país donde se encuentra la compañía, lo social, las decisiones políticas internas del país, la regulación o las leyes, la identificación financiera (cambios de precio del dólar), tecnológico, económico y ambiental [9], impulsores y tendencias claves que afectan los objetivos de la organización [10], relaciones, percepciones, valores, necesidades y expectativas de los grupos de interés externo [11], incluyen los proveedores y clientes, también las relaciones contractuales y compromisos con terceros, identificar la complejidad de las redes y dependencias. El contexto externo es todo lo relacionado donde puede la compañía impactar externamente o donde las situaciones externas le pueden causar algún impacto a la compañía.

El contexto Interno de la compañía, son los componentes que impactan desde adentro a la compañía cómo lo identifica el ISO 31000:2018: " la visión, la misión y valores de la compañía, el gobierno la estructura organizacional, los roles y

responsabilidades, la estrategia, los objetivos y políticas organizacionales, la cultura organizacional, los estándares, lineamientos y modelos adoptados por la organización, tecnología, capacidad económica, recursos, conocimiento, sistemas, datos, flujos y sistemas de información, relaciones interesadas internas cómo socios y grupos empresariales o socios de inversión, relaciones contractuales y compromisos, interdependencias e interconexiones (sucursales que se pueden encontrar en otros países pero que influyen en el contexto interno de la compañía)" [12].

Para identificar fácilmente el contexto de la compañía o el entorno, se encuentran herramientas cómo la matriz *DAFO*, que es el compuesto de *Debilidades*, *Amenazas*, *Fortalezas y Oportunidades*. Esta herramienta por medio de un cuadro identifica los factores internos y externos. En los factores internos se encuentran las *Fortalezas* y las *Debilidades* de la *Compañía*; en los factores externos se encuentran las Oportunidades y las Amenazas que también se menciona y se encuentran en los identificadores en el marco de referencia 5.4 de la ISO 31000:2018.

Figura 4- Cuadro de herramienta DAFO para identificar el contexto



Fuente: https://blog.epages.com/es/files/2016/07/Dafo-analisis.jpg

2) Identificación del contexto de usuario independiente (entorno): Para el caso de un usuario independiente, no se va a identificar ni hablar del contexto, esto con el fin de comunicar un lenguaje simple y estar en la posición de que el usuario independiente no está familiarizado con terminologías técnicas que puedan causarle algún tipo de confusión. El usuario independiente debe realizar una valoración del entorno en donde va a ser utilizado el dispositivo, este entorno debe validarlo externamente e internamente, lógico que al usuario independiente no se le debe poner a realizar un diagrama DAFO, pero si puede identificar fácilmente el entorno externo e interno con el proveedor que le ofreció el servicio, este debe suministrarle las respectivas indicaciones de utilización del dispositivo. Para ello, al igual que para identificar el contexto en una compañía cómo lo indica el marco de referencia 5 de la ISO 31000:2018, se debe identificar las debilidades y fortalezas del entorno en donde se va a encontrar el dispositivo o sistema.

Para identificar el entorno interno supongamos el siguiente escenario: Un usuario hace la adquisición de un dispositivo médico de IoT, dentro de las recomendaciones se encuentra que este dispositivo no puede estar al alcance de los niños, mucho menos se debe encontrar al alcance de mascotas y debe permanecer en un lugar higiénico; para esto, el usuario debe identificar las fortalezas y debilidades del lugar de su hogar y, debe recibir correctamente las recomendaciones que se le han indicado para uso óptimo del dispositivo o del servicio adquirido. Él empieza a hacer una valoración de su entorno interno, ósea en su hogar, esto con el fin de que pueda tener una correcta funcionalidad del sistema. Siguiendo con el escenario, al usuario también se le ha recomendado que el dispositivo debe encontrarse constantemente conectado al internet, para ello, le han indicado que el dispositivo puede realizar conexión a internet por señal LTE o de conexión inalámbrica cómo los que utiliza los celulares, también puede realizar una conexión a internet local por medio de internet wi-fi desde su hogar, si el usuario elige el servicio LTE, debe validar su entorno interno de que la señal de LTE tenga una buena cobertura en cualquier lugar de su hogar, pues puede encontrarse que el lugar que ha elegido para usar el dispositivo es el sótano y no es el lugar más óptimo para recibir una señal inalámbrica, pues puede encontrar una mala cobertura de señal para el dispositivo, para ello el usuario puede decidir que lo mejor es hacer uso de su red wi-fi, sin embargo, también debe hacer la valoración y encontrar el lugar o el entorno más óptimo en donde tiene mejor alcance de cobertura de la señal de wi-fi, y que el dispositivo no se encuentre bajo alguna amenaza que le cause algún riesgo de indisponibilidad. El usuario también debe hacer valoraciones financieras que se encuentren y se acomoden a su capacidad adquisitiva, pues puede generarle costos adicionales y no poder pagar por el uso de un sistema IoT.

La identificación del entorno interno, depende mucho de la manera de comunicación que le pueda proporcionar la asesoría en el momento de la compra del dispositivo, o las indicaciones dadas por el soporte de postventa del distribuidor de la marca o del fabricante.

Al igual, que para poder identificar el entorno interno se debe realizar la identificación del entorno externo, para ello se puede tomar como ejemplo la herramienta DAFO, que cómo lo indica en la figura 4 para la identificación de Factores externos se encuentran las oportunidades y las amenazas, para tal caso, el usuario debe identificar las oportunidades y amenazas que pueda tener el dispositivo que adquirió.

Un ejemplo de identificación de amenazas para determinar el contexto externo, es realizar una valoración del lugar en donde se encuentra el usuario, identificar las debilidades que pueden ocurrir en su vivienda y pueden afectar el dispositivo o el

servicio de IoT, tales como los constantes cortes de cableado que afectan disponibilidad del servido de internet, o si habita en un lugar en donde hay amenazas de inundación (pasa un rio cerca o vive junto a la playa). También debe validar con el fabricante, que el dispositivo tenga controles de seguridad en caso de recibir ataques que alteren la integridad del dispositivo y que los datos que transmite y recibe estén protegidos de malware, códigos maliciosos, de hombre en el medio o fallas que provengan de fábrica; incluso el usuario debe validar si se encuentra algún inconveniente legal el uso del dispositivo en su país de origen. Asimismo, para determinar el contexto externo, se debe evaluar las oportunidades que puede tener el usuario al hacer uso de un servicio de IoT, puede identificar todos los beneficios que puede obtener al haber adquirido el dispositivo, por ejemplo, ahorro de la tarifa de energía, mejor calidad de vida, ahorro de tiempo y etc.

B. Definir los criterios del riesgo

Tanto para las compañías que desean usar dispositivos IoT y el usuario independiente, debe primero definir los criterios del riesgo, identificando el alcance (hacia donde quieren llegar con el uso del dispositivo o servicio) y definir el objetivo (propósito del uso del dispositivo o servicio), tal y como se indicó anteriormente, las compañías al entrar a este mundo de IoT, deben definir sus políticas de seguridad de la información y contar con una adecuada gestión de riesgos, así mismo, el usuario o la compañía, debe tener claro el propósito de la adquisición de sus dispositivos, identificarlos cómo valores agregados para el mejoramiento del core de negocio, sus procesos y procedimientos.

Un usuario que haya adquirido un servicio o un dispositivo de IoT, en cambio, no se va a preocupar por una adecuada gestión de riesgos y mucho menos a definir sus riesgos, pues confía en el producto que le ofrecieron y por el cual adquirió pero, el distribuidor o las marcas de dispositivos que se encuentran ofreciendo IoT, deben tener claro el uso y la definición del riesgo que pueda tener el dispositivo en cualquier contexto, y adicional deben tener la responsabilidad de comunicar al usuario sobre el adecuado uso del dispositivo. El distribuidor de marca del dispositivo, debe realizar un análisis de seguridad al producto que va a ofrecerle al usuario, con características definidas con base y dependiendo de los criterios del riesgo.

La definición del riesgo se realiza de acuerdo al tipo de incertidumbre que puede afectar los resultados del objetivo [12], cómo afecta los objetivos de la compañía o del uso del dispositivo en caso de que se materialice el riesgo. Definir y medir las consecuencias en caso de que el riesgo se materialice [13], cómo se tendrán en cuenta las combinaciones y secuencias de riesgos múltiples [14].

V. EVALUACIÓN DEL RIESGO

Lo que indica la ISO31000:2018 evaluar el riesgo es identificarlo, se debe realizar el análisis de riesgo y la evaluación del riesgo [15], para realizar esta evaluación debe hacer una recolección de datos completos de una forma colaborativa con base al conocimiento y experiencia de las partes interesadas.

Los parámetros de *Evaluación del riesgo* para usuarios independientes, se realiza con base al objetivo que cumple el activo, en un sistema o proceso adquirido para una solución que contiene varios dispositivos asistidos entre sí, y que estén dentro de un sistema de IoT, entre los cuales, sistemas de dispositivos médicos, sistemas de hogares automatizados, sistemas de alarma o circuitos cerrados de televisión; incluyendo los recursos para el correcto funcionamiento del sistema, ejemplo: recursos económicos, canal de internet o de comunicación, módems de internet, páginas o aplicativos wep, aplicativos móvil, sensores, actuadores, y todo lo que defina o se determine cómo recurso para el correcto funcionamiento de sistemas de IoT.

A. Identificación del riesgo

La identificación del riesgo nos ayuda a encontrar y a reconocer los riesgos que podrían prevenir algún evento negativo para la compañía o para el usuario, se debe realizar la identificación de acuerdo al objetivo de un sistema o dispositivo de IoT.

Para identificar el riesgo debe hacer una correcta identificación del dispositivo o sistema, tener un objetivo claro de utilización del dispositivo y sus respectivos componentes que determinan el correcto funcionamiento del sistema o de un proceso IoT. Estos riesgos se pueden identificar de acuerdo a: indisponibilidad del sistema eléctrico, indisponibilidad del servicio del proveedor de Internet (LTE, Banda Ancha, etc), páginas web vulnerables de cross site scripting, latencias altas de respuesta de comunicación, páginas sin política de autenticación fuertes o de cambios de contraseña, actualizaciones del dispositivo, interrupciones por ataques DDos y botnets, cifrados, y aseguramiento de red local (módems inalámbricos o red wi-fi del hogar).

B. Método de Análisis del riesgo

El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características, poder determinar el nivel de riesgo, detalla las incertidumbres, las fuentes del riesgo, la probabilidad de ocurrencia del riesgo, eventos, las consecuencias del riesgo, escenarios, puede determinar sus controles [16] y así poder establecer los recursos para proteger el dispositivo o el sistema que compone los dispositivos de IoT.

Para realizar el análisis de riesgo, las empresas pueden decidir la metodología. En cambio, un usuario independiente puede adoptar las metodologías de una compañía, o que le comuniquen la identificación correcta de las probabilidades del riesgo por medio del distribuidor o proveedor del dispositivo o del sistema de IoT. A continuación se nombraran los pasos para el análisis de riesgo que deben realizar las compañías que eligen una solución de IoT, también este análisis sirve para los fabricantes de marcas que distribuyen dispositivos o servicios de IoT.

1) Inventario de activos: Para definir criterios del riesgo en una empresa debe realizar la identificación de los activos que compongan un servicio de IoT, para ello debe iniciar con un

inventario de activos que se encuentren dentro de un sistema ya sea automatizado o en un dispositivo. Para el caso de internet de las cosas, el activo puede ser el dispositivo o sus diferentes componentes del sistema de un servicio de IoT que haya adquirido un usuario independiente o una compañía.

Para el caso de las compañías, deben identificar en los activos la información que manejan y los servicios que prestan. Estos activos pueden estar enlazados a una información de base de datos de una compañía y estar en constante comunicación entre la nube y la intranet, puede estar en riesgo la disponibilidad, la integridad y la confidencialidad del sistema. Por lo tanto, este inventario no solo debe contener cantidades de activos que componen el sistema, también deben estar los servicios que prestan y que clase de información manejan.

Se debe dimensionar el dispositivo o activo a cuanto su confidencialidad, a su integridad y a su disponibilidad. La dimensión en cuanto a confidencialidad es el daño que causaría en caso de que lo conociera quien no debe, la dimensión en cuanto a Integridad es, que perjuicio causa si el dispositivo se encuentra dañado o corrupto, y en cuanto a disponibilidad, es que perjuicio causa de no tenerlo o no poderlo utilizar[17].

Para un usuario independiente, si decide un sistema de domótica en su hogar de IoT, muy seguramente todos los dispositivos incluyendo la nevera, la lavadora y hasta la licuadora, pueden estar enlazados entre sí, pues se encuentran dentro de un proceso automatizado, el distribuidor que le suministre este servicio, debe de explicarle al usuario el servicio adquirido, entregarle un inventario de todos los componentes y dispositivos que se encuentran en la red de domótica de su hogar, identificando en cada uno de ellos la información y los servicios que cada uno presta. Por lo tanto, no es desmedido pensar, que un usuario debe estar en la capacidad de entender y de conocer el inventario que compone su sistema de IoT.

2) Valoración de los activos: después de haber identificado los activos, y haber realizado el inventario, se empieza a darles una valoración, no solo se habla del costo monetario del dispositivo si no de la importancia del activo, identificar aquel activo que genera un valor mayor que otro dependiendo de la importancia del proceso, por lo tanto, esta valoración se debe dar de acuerdo a una perspectiva de la necesidad de proteger el dispositivo, este valor es proporcional a la protección del activo esto quiere decir, cuanto mayor sea el valor del activo mayor es la protección que va a recibir el activo, también se debe tener encueta que la valoración de estos activos están totalmente relacionados con la identificación del contexto interno y externo de la organización, y también con la valoración del entorno externo e interno realizado por el usuario independiente.

El valor del activo puede ser cualitativa o cuantitativa. Los valores Cualitativos son valores descriptivos que se dan de acuerdo a la cualidad y características del dispositivo, sus valores son dependiendo de la percepción de seguridad que le pueda dar el usuario, ya sean *Alta, Media, Bajo o Muy Bajo*.

El valor cuantitativo que se le asignan al activo corresponden a valores numéricos que se le dan al activo de acuerdo al costo monetario que implica en caso de alguna eventualidad de daño o de degradación del activo, tal y como lo indica la *Metodología de Magerit* "Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero permiten sumar valores numéricos de forma absolutamente "natural". La interpretación de las sumas no es nunca motivo de controversia."[18] Sin embargo, se deben hacer análisis de costos o estudios económicos comparando con lo que se arriesga con respecto a lo que puede costar la solución o control para proteger el activo.

3) Amenazas: luego de haber realizado una valoración de activos, ahora se debe determinar las amenazas que pueden afectar a cada dispositivo o sistema que comprende el IoT. Para ello, se deben identificar las amenazas que pueden ser de, tipo natural, del entorno, causadas de forma accidental o de forma deliberada.

Las Amenazas de tipo de natural, son aquellas que son de eventos causados por el medio ambiente y son peligrosos para las personas (Terremotos, inundaciones, huracanes, incendios forestales, tormentas, etc).

Amenazas del entorno, son los causados por elementos que pueden afectar al sistema o al dispositivo por ejemplo, en el hogar o en una empresa: conexiones de gas, conexiones eléctricas, recipientes de agua que se puedan derramar cerca al dispositivo, elementos químicos, fallos eléctricos o contaminantes.

Las amenazas de tipo accidental, son aquellas en las que puede estar en lugares no permitidas para las personas o en ellas pueda haber algún tipo de manipulación no intencionados que puedan indisponer el servicio, ya sea por omisión o por error.

Y por último están aquellas amenazas de forma deliberada, son aquellas que pueden tener acceso a un sistema o permisos de ingreso al dispositivo, y pueden causar problemas intencionados para beneficio propio o solo por causar daños, ejemplo: un atacante puede realizar cambios de contraseña o cambios de segmentación de red, con el fin de dejar sin disponibilidad a los usuarios del sistema, mientras, el atacante puede recoger información confidencial o simplemente causar el daño a la compañía por el tiempo que estuvo indisponible el sistema.

4) Valoración de las amenazas: así mismo cómo la valoración que se les realiza a los activos, se debe hacer una valoración a las amenazas que pueda presentar el activo, esta valoración se puede hacer dependiendo de la probabilidad de ocurrencia de la amenaza (ideal para la valoración de amenazas de tipo natural) o por degradación (cuán perjudicado resultaría el valor del activo) [19].

La degradación mide un daño causado por el incidente en el supuesto de que ocurriera [20]. Después de que un incidente haya sucedido, el activo o dispositivo no se ha degradado totalmente.

La probabilidad de ocurrencia no es fácil de determinar o de expresar, se modela cualitativamente por medio de una tabla nominal [21].

TABLA I. DEGRADACIÓN DE VALOR DE DAÑO

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Fuente: Magerit, valoración de amenazas

También se da una modelación numérica, calificando la probabilidad de ocurrencia de la amenaza, la orientación puede ser con base al tiempo, ejemplo: la probabilidad de que ocurra una inundación es cada año en temporada de invierno, o es frecuentemente que ocurra una inundación cada vez que llueve. Para identificar la probabilidad de ocurrencia, se puede realizar una tabla que le permita identificar la frecuencia de que probablemente ocurra una eventualidad para así poder valorar la amenaza, tal y como se muestra en *Tabla II probabilidad de ocurrencia*.

TABLA II. PROBABILIDAD DE OCURRENCIA

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Fuente: Magerit, valoración de amenazas

Un usuario independiente, por lo general no se preocupa por las amenazas, él depende del servicio o dispositivo que le haya ofrecido el distribuidor de su producto, o del fabricante del dispositivo del sistema de IoT, por eso los fabricantes deben garantizar la calidad de lo que ofrece y siempre deben orientar al usuario de las amenazas de seguridad que pueden tener los dispositivos o servicios que ofrezcan.

5) Determinación del impacto: es el daño ocasionado al activo producido por la materialización de la amenaza. Este valor se obtiene conociendo el valor del activo y la degradación que le causaría la amenaza, deriva el impacto que tendrían sobre el sistema o sobre el propio activo, en este punto se debe pensar que el impacto ya ha perjudicado la confidencialidad, la integridad y la disponibilidad del activo.

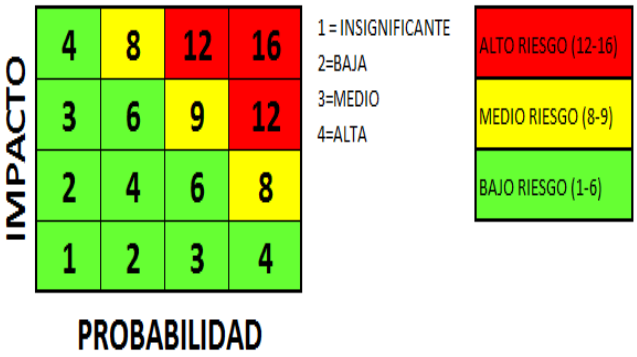
6) Impacto acumulado: es el valor calculado sobre un activo, depende de la información que puede manejar de sí mismo o de otros dispositivos o activos que depende de él. Un impacto es mayor cuando el valor del activo es mayor si este activo depende de varios sistemas, el impacto para este activo es mayor, pues el daño ocasionado al activo puede dejar sin disponibilidad el sistema que depende de él. Un escenario es que se dañe el servidor central de IoT, el impacto que tendría es muy alto, debido a que el servidor central o gateway, se puede comunicar con otros subsistemas que contienen muy posiblemente varios dispositivos que componen un sistema automatizado.

7) Impacto repercutido: Es aquel Impacto que puede afectar a otros sistemas adicionales o a otros activos, y ayuda a determinar las consecuencias de las incidencias técnicas.

8) Determinación del riesgo: "Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia" [22].

El riesgo es en función del impacto y la probabilidad, analizando el cuadro de la figura 5, muestra en la zona roja que entre más alta es la probabilidad y más alto sea el impacto el riesgo es mayor. La zona amarilla corresponde a un riesgo medio, y por último esta la zona verde, que indica un riesgo es bajo cuando la probabilidad es baja y el impacto es alto, o cuando el impacto es alto pero la probabilidad es baja.

Figura 5- Cuadro de determinación del riesgo



Fuente: El autor

9) Controles: ya cuando se ha determinado el riesgo, se puede identificar la clase de controles o salvaguardas que se deben de aplicar a cada uno de los activos que componen el sistema de IoT. Estos controles también pueden tener un costo monetario o de algún tipo que genere valor, no solo deben estar sujeto al valor del activo, si no también, a los daños materiales que pueden causar si no se llegarana proteger de algún riesgo al activo.

Los controles son importantes debido a que pueden reducir la probabilidad de ocurrencia, reducir de un impacto mayor o de un riesgo alto. Estos controles que mitigan el riesgo pueden ser de tipo preventivo tales como, la autorización de privilegio de usuario, controles disuasivos (cámaras de circuito cerrado de televisión o vallas y mensajes de peligro), eliminativos, controles que minimizan el impacto o limitan el impacto, correctivos (sistemas redundantes de comunicaciones o de líneas eléctricas), controles de recuperación (back-ups), también pueden ser de monitoreo o registros de eventualidades, controles que puedan detectar algún tipo de evento (antivirus, IDS´s), controles de concienciación (capacitaciones), o controles administrativos (análisis de riesgo, y planes de continuidad de negocio).

C. Evaluar el riesgo

La evaluación del riesgo, apoya a la toma de decisiones con respecto al riesgo y compara los resultados del análisis de riesgo realizado por la compañía, mientras el usuario independiente, debe evaluar el riesgo determinando los lugares que se requieren tomar algún tipo de acción preventiva, esto es para minimizar los eventos negativos que le puedan causar al sistema.

La evaluación ayuda a decidir qué hacer con el riesgo como lo indica la *ISO 31000:20018*: "a no hacer nada, considerar opciones para tratar el riesgo, realiza análisis adicionales para comprender mejor el riesgo, mantener los controles existentes, reconsiderar los objetivos de la empresa" [23].

Estas acciones deben ser determinadas de acuerdo al contexto realizado por la empresa, y que no contenga consecuencias a los objetivos de la compañía o del uso del sistema adquirido. Con la evaluación del riesgo se puede concluir si el riesgo es inherente o residual.

Un riesgo Inherente es aquel riesgo que no se puede eliminar y al realizarlo puede influir negativamente en los objetivos de la compañía o de algún sistema adquirido para el uso del IoT, este riesgo es propio del proceso, quiere decir que es un riesgo con el cual va estar presente [24].

El riesgo residual es un riesgo latente después de implementar los debidos controles, aunque el riesgo es imposible de ser radicado, si se debe encontrar el equilibrio entre los recursos y mecanismos que mitiguen o reduzcan el riesgo. Este riesgo es aquel que permanece después de que la alta dirección desarrolle su respuesta a los riesgos [25].

VI. TRATAMIENTO DEL RIESGO

El tratamiento de riesgo implementa las acciones que se deben realizar para abordar el riesgo cuando son aceptados, transferidos, cuando se pueden evitar o eliminar. Se deben formular y seleccionar opciones de tratamiento de riesgo, planificación e implementación de tratamiento de riesgos, evaluar la efectividad de ese tratamiento, decidir si el riesgo restante es aceptable, si no es aceptable, tomar tratamiento adicional [26].

A) Acciones de riesgo

1) Aceptación del riesgo: Un riesgo aceptado es el que se va a asumir, coloquialmente " se corre el riesgo" y es que a veces es mejor aceptar el riesgo, pues puede salir más costoso eliminarlo, sin embargo, si se realizó una adecuada gestión del riesgo, es la compañía o el usuario que tiene la capacidad de aceptarlo, porque puede que el costo no sea tan alto de acuerdo al daño causado, es un riesgo residual que no pudo ser eliminado y debe ser asumido por la compañía o por el usuario de IoT.

Para ello se le puede dar el siguiente tratamiento: prestar nuevos servicios o trabajar una nueva información, alterar la arquitectura del sistema, reduciendo controles porque implican mayores costos o reducir el endurecimiento de los controles.

2) Transferir el riesgo: Este riesgo es aquel que por costes de los controles no pueden ser asumidos por la propia compañía o por algún usuario de IoT, para esto, el riesgo se pasa a una entidad externa que mediante un estudio de costos, sale un poco más barato que asumirlo el propietario del activo. Este riesgo puede ser transferido a modalidad de outsursing, o lo puede cubrir una entidad aseguradora, esta medida solo cubrirá cierta parte de daños ocasionados de una materialización del riesgo, es una opción paliativa. En caso de una eventualidad, el daño no va a ser cubierto totalmente y debe ser definido por medio de un contrato, que delimite las responsabilidades que deben asumir el tercero y la aceptación del alcance del dueño del propietario del activo.

Para los usuarios independientes, deben ser concienciados por medio del distribuidor de la marca, indicando cual es el alcance de responsabilidades tanto del propietario cómo del proveedor, así mismo, esto depende del sistema adquirido para una correcta manipulación del dispositivo o sistema que se encuentre en el IoT.

3) Evitar el riesgo: Un riesgo evitado es aquel que puede ser mitigado o degradado para reducir la ocurrencia del evento negativo por medio de salvaguardas más fuertes.

Se debe tener cuidado y discreción en la implementación de endurecimiento de controles, pues estos salvaguardas pueden afectar el sistema o el automatismo de los dispositivos del sistema de IoT, se puede presentar que las actualizaciones de firmware que se le realice al dispositivo (sean sensores o actuadores) puede degradar el sistema, para ello, los acuerdos de responsabilidades de endurecimiento a los sistemas de IoT, deben ser claros y entendidos por las partes interesadas y que no afecten el objetivo del proceso.

4) Eliminar el riesgo: el riesgo eliminado es aquel riesgo que por costos no puedan ser asumidos o transferidos por los propietarios de los activos, deben alejarse del riesgo; debido a que ese riesgo puede ocasionar afectación al contexto interno y externo de la compañía o del proceso del sistema que se esté utilizando, asimismo para eliminar el riesgo, puede hacer modificaciones a los objetivos de la compañía o de los objetivos del proceso del sistema ofrecido por los distribuidores y fabricantes de las marcas de IoT.

B) Plan de tratamiento de riesgos

El objetivo de armar un plan de tratamiento de riesgo, es identificar con las partes interesadas quien va a ser el responsable de implementar el tratamiento para mitigar el riesgo, y que los resultados de dichos controles sean efectivos para la compañía o para el producto ofrecido por el distribuidor o fabricante de IoT. En caso de los usuarios independientes, deben tener claridad de los sistemas de IoT adquiridos y aceptar las recomendaciones e indicaciones del correcto funcionamiento realizadas por los fabricantes y distribuidores de IoT.

En caso de algún tipo de eventualidad con un sistema o dispositivo de IoT, el usuario debe identificar como y a quien se le puede dirigir el incidente, ya sean por medio de los canales de comunicación suministrados por los distribuidores o fabricantes de marcas, o acuerdos de niveles de atención a fallas.

.

VII. MONITOREO Y REVISIÓN

El monitoreo y revisión de la gestión del riesgo sirve para mejorar la calidad y efectividad del proceso [26], este monitoreo puede ser realizado por medio de auditorías a los procesos y procedimientos que se encuentren en el análisis de eventualidades de seguridad encontradas, para las compañías que hayan adquirido sistemas y dispositivos de IoT, se deben regir y alinear a las políticas de seguridad de la información internas, preferible y no obligatorias, que cuenten con sistemas de Gestión de Seguridad de la Información y que tengan en su política la revisión constante de los sistemas de IoT.

Para los usuarios independientes, deben contar con la información necesaria suministrada por el distribuidor de la marca o fabricante que le ofrecen un sistema o dispositivo de IoT; el usuario debe ser informado, que su producto cuenta con un debido control de seguridad de la información y que este se encuentra en constante revisión para la protección de su información. Estas empresas distribuidoras deben planificar y suponer que el usuario no cuenta con el suficiente conocimiento de manejo de protección de sus datos, por lo tanto, el distribuidor o la marca, se hace responsable de daños ocasionados a los sistemas, claro está, esto depende del sistema adquirido por el usuario y del riesgo que pueda tener este dispositivo o sistema de servicio IoT.

VIII. REPORTES E INFORMES

La gestión de riesgos y sus resultados deben ser documentados y también ser informados [27], esto con el fin de encontrar evidencias de eventualidades e incidentes para poder realizar a su sistema mejoras, se debe realizar con mecanismos apropiados, por ejemplo, revisar los logs de eventos reportados por los sistemas monitoreados, logs de procesos de los dispositivos de los servicios de IoT, deben informar sus resultados a las partes interesadas (usuarios y propietarios del riesgo), proporcionar información para la tomas de decisiones, en especial para aquellos usuarios independientes que posiblemente pueda desistir de algún sistema o dispositivo que cuenten con servicio de IoT, por motivos de costos de actualización de los dispositivos o servicios contratados.

Estos informes también brindan la oportunidad de mejorar actividades de gestión de riesgos, muy posible con el tiempo haya una degradación del riesgo y se tenga que cambiar alguna actividad de procedimiento de controles, debe ser siempre con base al objetivo del sistema o de la compañía y también ser informado a las partes interesadas para su aprobación o su derogación.

IX. CONCLUSIONES

El éxito de la utilización de los servicios del internet de las cosas, depende de la confianza que le brinda a sus usuarios el distribuidor o el fabricante de marcas de dispositivos y servicios de IoT, dependiendo de sus políticas de Gestión de Seguridad de la Información internas, ayudaran a una correcta protección de sus dispositivos o sistemas, que en percepción por estar en la nube, no muchos usuarios consideran seguros y piensan que su información se encuentre en riesgo.

Nadie quiere adquirir un servicio o producto que no le brinde la mayor seguridad, que pueda estar expuesta su intimidad y se convierta en víctima de chantajes económicos o degradan de su personalidad por motivos de ciber bullyng o extorsión sexual; cada día se extiende el uso del internet, y la información de cada usuario se puede consultar desde cualquier lugar del mundo, por eso, se deben crear estrategias que puedan garantizar la protección de la integridad, la disponibilidad y la confidencialidad de la información y de aquellos sistemas y dispositivos que utilizan los servicios de IoT.

Asimismo, la importancia de informar y distribuir sistemas que permitan proteger la información y puedan concientizar el correcto uso de los servicios y dispositivos, difundir y comunicar a los usuarios de que nadie esta excepto de riesgos cuando se adquiere un servicio de IoT.

Los pasos y los principios de la seguridad de la información son ideales para mantener una adecuada protección de sus datos y así, asegurar la información que pueda tener algún tipo de vulnerabilidad.

Para realizar una adecuada Gestión de Riesgos de IoT, se recomienda documentación de estándares reconocidos de sistemas de gestión de la seguridad (SGSI) entre los cuales: Iso 27001:2013, *Gestión de Riesgos ISO 31000:2018* y controles necesarios y técnicas para la protección de los datos en la nube por ejemplo: la ISO 27018:2019, mencionadas para la realización de este artículo. Se debe también contar con el uso de metodologías cómo *Magerit*, para realizar un correcto análisis de riesgos e identificar correctamente los riesgos y vulnerabilidades que contengan la compañía o el usuario del IoT.

REFERENCIAS

[1] G. Coser, “Internet of things (IOT) Secure best practice”, pp. 2, Feb, 2017

[2] M. C Maria Alejandra. (2017, Oct, 5), "La historia detrás de la internet de las cosas" [Online]. Available: https://www.elespectador.com/tecnologia/la-historia-detras-de-la-internet-de-las-cosas-articulo-716678

[3] H.N Security. (2019, Jun, 21), "41.6 billion IoT devices will be generating 79.4 zettabytes of data in 2025" [Online]. Available: https://www.helpnetsecurity.com/2019/06/21/connected-iot-devices-forecast/

[4] IDC. (2019, Jul, 15) "New IDC Forecast Expects the Internet of Things Spending in Asia/Pacific* to Reach USD 398.6 Billion by 2023" [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prAP45362119

[5] ISO/IEC27001:2005. (2013), "Information security risk assessment” vol.2, no. ISO27001:2013, pp.7, Noviembre 2013.

[6] ISO/IEC27001:2005. (2013), "Information security risk treatment” vol.2, no. ISO27001:2013, pp.7, Noviembre 2013.

[7] ISO/IEC27001:2005. (2013), "Context of the organization" vol.2, no. 27001:2013, pp.1, Noviembre 2013.
[8] ISO/IEC 31000:2018, "Understanding the organization and its context". vol. 2, no. ISO31000:2018, pp.6, Feb.20
[9] ISO/IEC 31000:2018, "Understanding the organization and its context". vol. 2, no. ISO31000:2018, pp.6, Feb.20
[10] ISO/IEC 31000:2018, "Understanding the organization and its context". vol. 2, no. ISO31000:2018, pp.6, Feb.20
[11] ISO/IEC 31000:2018,"Gestion de Riesgo".ISO, Feb.2018.
[12] ISO/IEC31000:2018, "Defining risk criteria" vol.2, no. ISO31000:2018, pp.10, 11, Feb. 2018.
[13] ISO/IEC31000:2018, "Defining risk criteria" vol.2, no.ISO31000:2018, pp.10, 11, Feb. 2018.
[14] ISO/IEC 31000:2018, "Defining risk criteria" vol.2, no. ISO31000:2018, pp.10, 11, Feb.2018.
[15] ISO/IEC31000:2018, "Risk assessment" vol.2, no. ISO31000:2018, pp.11, Feb.2018
[16] ISO/IEC31000:2018, "Risk analysis" vol.2, no. ISO31000:2018, pp.12, Feb.2018
[17] Magerit,"Metodología de análisis y gestión de riesgos" vol.3,no.630-12-171-8, pp.24, Oct 2012
[18] Magerit,"Metodología de analisis y gestion de riesgos" vol.3, no.630-12-171-8, pp.26, Oct 2012
[19] Magerit,"Metodología de analisis y gestion de riesgos" vol.3, no.630-12-171-8, pp.28, Oct 2012
[20] Magerit,"Metodología de analisis y gestion de riesgos" vol. 3, no. 630-12-171-8, pp. 28, Oct 2012
[21] Magerit,"Metodología de analisis y gestion de riesgos"vol.3,no.630-12-171-8,pp.28,Oct 2012
[22] Magerit,"Determinación del riesgo potencial" vol.3, no.630-12-171-8, pp. 29, Oct 2012
[23] ISO/IEC31000:2018, "Risk evaluation" vol.2, no. ISO31000:2018, pp. 12, Feb.20
[24] I. rodríguez. (2014, Nov, 18), " ¿Qué es el riesgo, riesgo inherente y riesgo residual?" [Online]. Available: https://www.auditool.org/blog/control-interno/3073-que-es-el-riesgo-riesgo-inherente-y-riesgo-residual
[25] I. Rodríguez. (2014, Nov, 18), "¿Qué es el riesgo, riesgo inherente y riesgo residual?" [Online]. Available: https://www.auditool.org/blog/control-interno/3073-que-es-el-riesgo-riesgo-inherente-y-riesgo-residual
[26] ISO/IEC31000:2018, "Monitoring and review" vol. 2, no. ISO31000:2018, pp.14, Feb.20
[27] ISO/IEC31000:2018, "Recording and reporting" vol. 2, no. ISO31000:2018, pp.14, Feb.20

Autor. Gantiva Henao Luis Alexander, Nació en la ciudad de Bogotá el 22 de julio de 1981, Ingeniero Electrónico de la Universidad Incca de Colombia en el 2008 y Estudiante de Especialización en Seguridad Informática de la Universidad Piloto de Colombia en el 2019. Cuenta con más de 9 años de experiencia en arquitectura de red, configuración y seguridad de redes, y en plataformas de seguridad informática, su experiencia laboral ha sido en empresas del área financiera y logística.